Amendments to the Claims

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1.   (Original) A method for encrypting an electronic message composed by a sender using an abbreviated address book for delivery over a mail system to a recipient who holds a digital certificate, comprising:

    (a)   when the sender is off-line, inserting an encryption flag in a header associated with the electronic message;

    (b)   placing the header and the message in plain text in an outbox;

    (c)   when the sender is on-line, in response to the flag, requesting the digital certificate from the mail system; and

    (d)   using the received certificate to encrypt the plain text mail message.

2.   (Original) The method according to claim 1 further comprising:

    (e)   sending the encrypted mail message to the mail system.

3.   (Currently Amended) The method according to claim 1 further comprising:

    [[(f)]](e)   when the sender is on-line, if the flag indicates that the message is encrypted, sending the encrypted mail message to the mail system.

4.   (Original) The method according to claim 1 wherein step (c) comprises:

    (c1)   requesting the digital certificate from the mail system; and

    (c2)   if the certificate is unavailable, informing the sender that the message cannot be encrypted.

5.   (Currently Amended) The method according to claim 4 further comprising:

[[(a)]] (e)   sending the unencrypted mail message in the outbox to the mail system when the message cannot be encrypted.

6.   (Currently Amended) The method according to claim 1 wherein the header comprises information identifying the recipient and step (c) comprises:

[[(c3)]] (c1)   using the identifying information to locate the recipient in the mail system and to retrieve the certificate.

7.   (Original) Apparatus for encrypting an electronic message composed by a sender using an abbreviated address book for delivery over a mail system to a recipient who holds a digital certificate, comprising:

a mail composer which inserts an encryption flag in a header associated with the electronic message when the sender is off-line;

a sending mechanism which places the header and the message in plain text in an outbox;

a verification mechanism which is operable when the sender is on-line and, in response to the flag, requests the digital certificate from the mail system; and

an encryption mechanism which uses the received certificate to encrypt the plain text mail message.

8.   (Original) The apparatus according to claim 7 further comprising:

an outbox mechanism which sends the encrypted mail message to the mail system.

9.   (Original) The apparatus according to claim 7 further comprising:

a mail mechanism which operates when the sender is on-line and, if the flag indicates that the message is encrypted, sends the encrypted mail message to the mail system.

10.   (Original) The apparatus according to claim 7 wherein the verification mechanism comprises:

a mechanism which requests the digital certificate from the mail system; and

warning apparatus which informs the sender that the message cannot be encrypted if the certificate is unavailable.

11.   (Previously Amended) The apparatus according to claim 10 further comprising:

an outbox mechanism which sends the unencrypted mail message in the outbox to the mail system when the message cannot be encrypted.

12.   (Original) The apparatus according to claim 7 wherein the header comprises information identifying the recipient and wherein the verification apparatus comprises:

a locator which uses the identifying information to locate the recipient in the mail system and to retrieve the certificate.

13.   (Original) A computer program product for encrypting an electronic message composed by a sender using an abbreviated address book for delivery over a mail system to a recipient who holds a digital certificate, the computer program product comprising a computer usable medium having computer readable program code thereon, including:

program code operable when the sender is off-line, for inserting an encryption flag in a header associated with the electronic message;

program code for placing the header and the message in plain text in an outbox;

program code operable when the sender is on-line and, in response to the flag, for requesting the digital certificate from the mail system; and

program code for using the received certificate to encrypt the plain text mail message.

14.   (Original) The computer program product according to claim 13 further comprising:

program code for sending the encrypted mail message to the mail system.

15. (Original) The computer program product according to claim 13 further comprising:

program code operable when the sender is on-line and, if the flag indicates that the message is encrypted, for sending the encrypted mail message to the mail system.

16. (Original) The computer program product according to claim 13 wherein the program code for requesting the certificate comprises:
program code for requesting the digital certificate from the mail system; and
program code for informing the sender that the message cannot be encrypted, if the certificate is unavailable.

17. (Original) The computer program product according to claim 16 further comprising:

program code for sending the unencrypted mail message in the outbox to the mail system when the message cannot be encrypted.

18. (Original) The computer program product according to claim 13 wherein the header comprises information identifying the recipient and the program code for requesting the certificate comprises:

program code for using the identifying information to locate the recipient in the mail system and to retrieve the certificate.

19. (Original) A computer data signal embodied in a carrier wave for encrypting an electronic message composed by a sender using an abbreviated address book for delivery over a mail system to a recipient who holds a digital certificate, the computer data signal comprising:

program code operable when the sender is off-line, for inserting an encryption flag in a header associated with the electronic message;

program code for placing the header and the message in plain text in an outbox;

program code operable when the sender is on-line and, in response to the flag, for requesting the digital certificate from the mail system; and

program code for using the received certificate to encrypt the plain text mail message.

20. (Original) The computer data signal according to claim 19 further comprising: program code for sending the encrypted mail message to the mail system.